Fig. 1

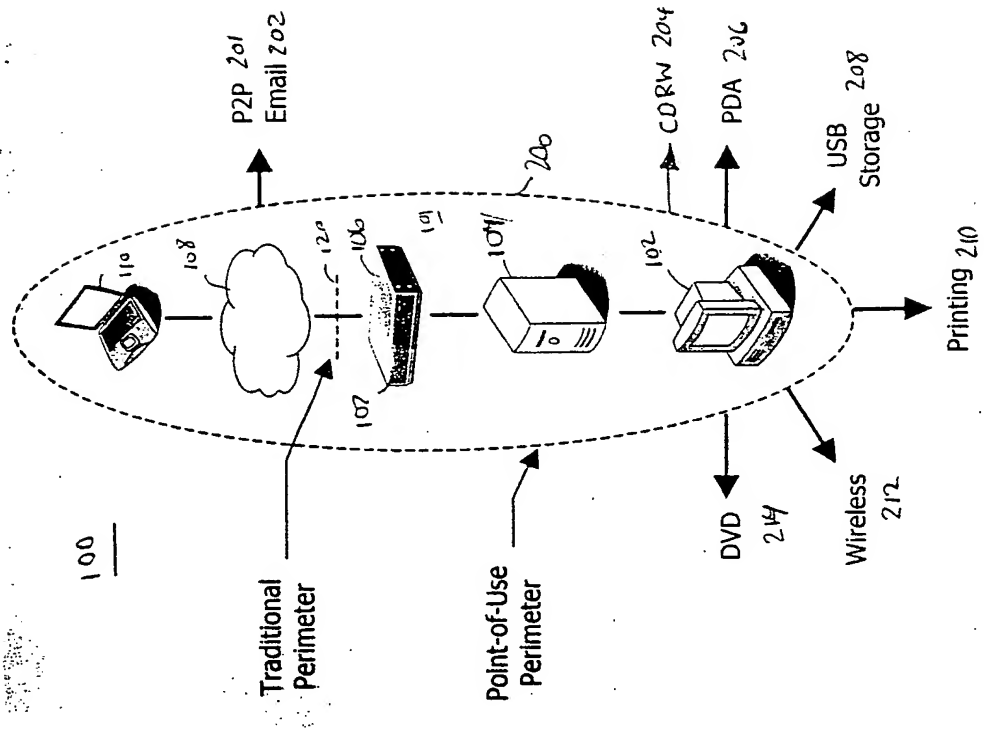
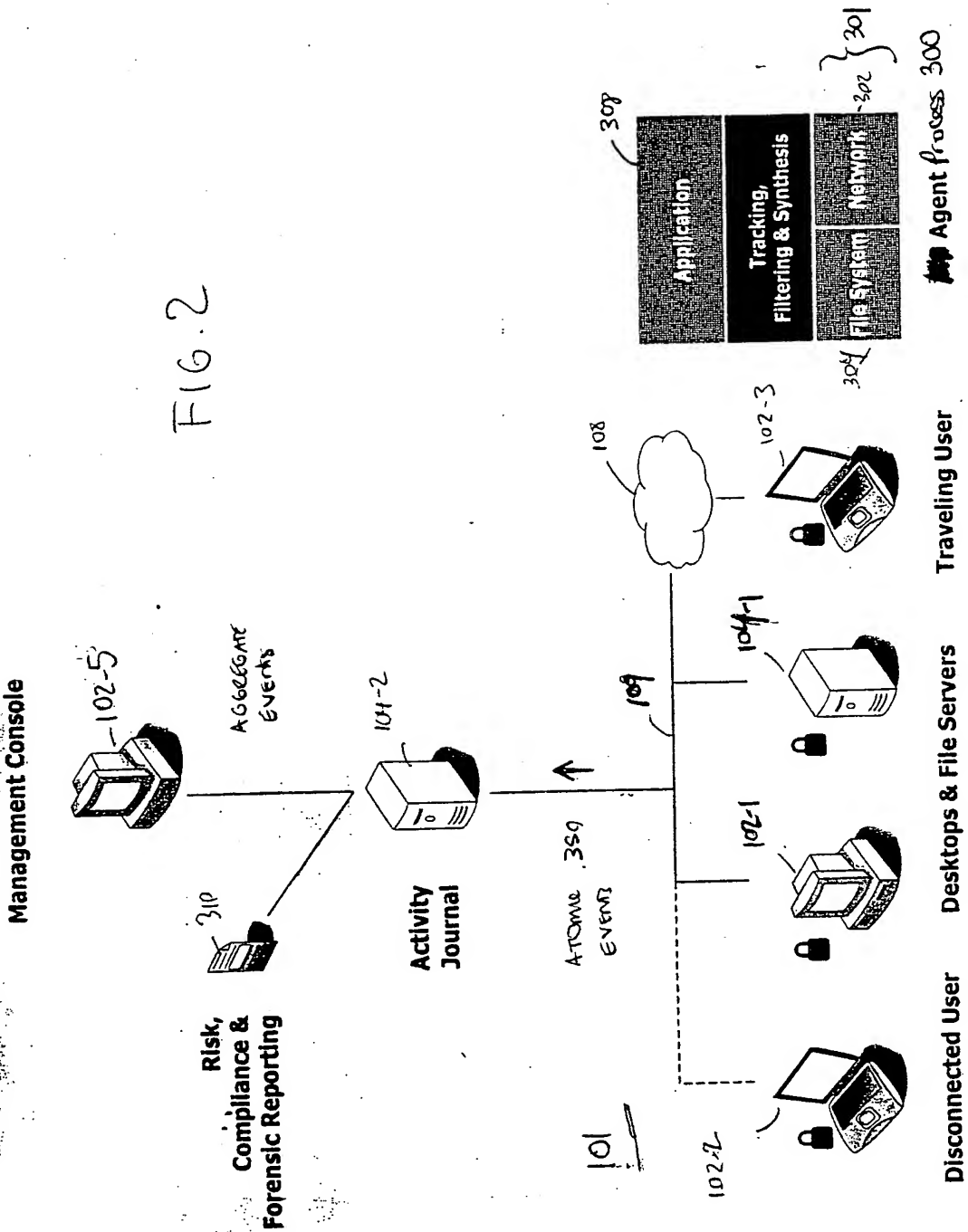

P2P 201
Email 202
CDRW 204
PDA 206
USB Storage 208
Printing 210
DVD 214
Wireless 212
Traditional Perimeter
Point-of-Use Perimeter
100
200

FIG. 2


Management Console
102-5
Aggregate Events
101-2
Activity Journal
310
Risk, Compliance & Forensic Reporting
Atomic Events 309
108
102-3
Traveling User
101-1
Desktops & File Servers
102-1
Disconnected User
102-2
101
Agent process 300
301
302
Application
Tracking, Filtering & Synthesis
File System
Network
304

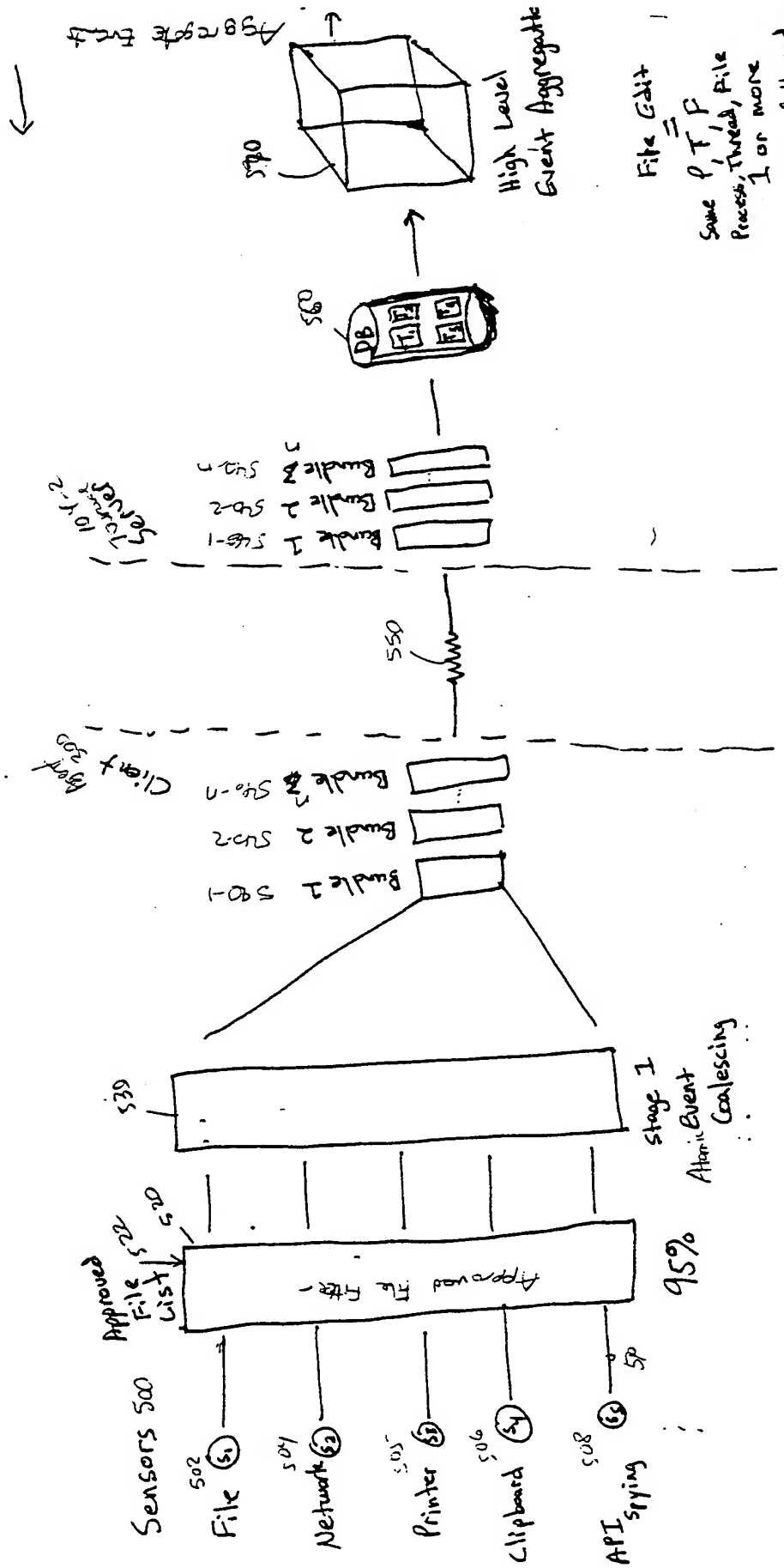

Sensors 500
File 502
Network 504
Printer 506
Clipboard 508
API Spying
Approved File List 520
Approved File Files
Stage 1 Atomic Event Coalescing
539
95%
Bundle 1 Seq-1
Bundle 2 Seq-2
Bundle n Seq-n
Client Side
Server Side
550
DB
560
High Level Event Aggregate
570
File Edit = Same P, F, F Process, Thread, File 1 or more reads followed by a write

FIG. 3

Atomic Events

Action Type	Level	Event Category	Event Name	Event Table	Action Detail Field	Action Detail Value	Discriminant
1	Low	File	FileRead	FileEvent	operationType	0	bytesRead > 0, bytesWritten = 0
2	Low	File	FileWrite	FileEvent	operationType	0	bytesRead = 0, bytesWritten > 0
3	Low	File	FileReadWrite	FileEvent	operationType	0	bytesRead > 0, bytesWritten > 0
4	Low	File	FileCopy	FileEvent	operationType	1	
5	Low	File	FileRename	FileEvent	operationType	2	
6	Low	File	FileDelete	FileEvent	operationType	3	
7	Low	File	FileMove	FileEvent	operationType	4	
8	Low	File	FileRecycle	FileEvent	operationType	5	
9	Low	File	FileRestore	FileEvent	operationType	6	
10	Low	Network	TCPIPInbound	NetworkEvent	protocolType	TCPIP	isOutbound = 0
11	Low	Network	TCPIPOutbound	NetworkEvent	protocolType	TCPIP	isOutbound = 1
12	Low	Network	UDPInbound	NetworkEvent	protocolType	UDP	isOutbound = 0
13	Low	Network	UDPOutbound	NetworkEvent	protocolType	UDP	isOutbound = 1
14	Low	Network	IPSECInbound	NetworkEvent	protocolType	IPSEC	isOutbound = 0
15	Low	Network	IPSECOutbound	NetworkEvent	protocolType	IPSEC	isOutbound = 1
16	Low	Print	Print	PrintEvent	(Implied)	N/A	
17	Low	CD	CDRead	CDEvent	operationType	1	
18	Low	CD	CDWrite	CDEvent	operationType	2	
19	Low	Clipboard	ClipboardCutCopy	ClipboardEvent	eventType	CutCopy	
20	Low	Clipboard	ClipboardPaste	ClipboardEvent	eventType	Paste	
21	Low	User	UserLogon	UserEvent	eventType	Logon	
22	Low	User	UserLogoff	UserEvent	eventType	Logoff	
23	Low	Machine	Machine	MachineEvent	eventType	***	Skip the Machine events.
24	Low	Process	ProcessStart	Process	(Implied)		Use processStartDtTm
25	Low	Process	ProcessEnd	Process	(Implied)		Use processEndDtTime
26	High	File	FileEdited	AggregateEvent			
27	High	File	FileCopied	AggregateEvent			
28	High	File	FileSaveAs	AggregateEvent			
29	High	File	FileLeftThroughRemovableMedia	AggregateEvent			
30	High	Clipboard	ClipboardToFile	AggregateEvent			
31	High	Print	PrintFile	AggregateEvent			
32	High	CD	BurnMaster	AggregateEvent			
33	High	CD	BurnFile	AggregateEvent			
34	High	Network	FileLeftThroughNetworkPort	AggregateEvent			
35	High	Network	EmailFile	AggregateEvent			
36	High	Network	RemoteAccess	AggregateEvent			
37	High	Network	InstantMessenger	AggregateEvent			
38	High	Network	P2PApp	AggregateEvent			
39	High	Network	FTPFile	AggregateEvent			
40	High	Network	TunnelOut	AggregateEvent			
41	High	Network	TunnelIn	AggregateEvent			
42	High	Network	TunnelInOut	AggregateEvent			
43	High	Network	FileOutThroughTunnel	AggregateEvent			

FIG. 4

Aggregate Event Definitions

Event Name	Constituent Event Types	Pattern	Scope
FileEdited	FileRead, FileWrite, FileReadWrite	Same processId and fileHandle. beforeHash of first read & afterHash of last write differ. Both reads and writes to same fileHandle. Sum of writes > 0.	Thread
FileCopied	FileRead, FileWrite, FileReadWrite, FileCopy	Command shell: Alternating reads & writes. The reads all have one filehandle, the writes all have a second one. Explorer: A long series of reads from one filehandle followed by a long series of writes to a second. Mind the time period between. In both cases, the target device must not be removable.	Thread
FileSaveAs	FileRead, FileWrite, FileReadWrite	An app reads one or more files then writes a file	Process
FileLeftThroughRemovableMedia	FileRead, FileWrite, FileReadWrite, FileCopy	Same as FileCopied or FileSaveAs, but target device is removable.	Process
ClipboardToFile	ClipboardCutCopy, ClipboardPaste	Pair a ClipboardCutCopy with all subsequent ClipboardPaste events for that user login until the next copy or the user logs out. Problem: If the user closes the application that performed the copy and the object was large and the user opts not to keep it there, what happens?	Login
PrintFile	Print, possibly others	Unclear. If there are temp files, intermediate PDF files, etc, then we may perform a chain of custody analysis to figure out just what was printed.	Thread
BurnMaster	FileRead, FileWrite	An app known to burn files reads one or more files then writes a file.	Process
BurnFile	CDWrite, FileRead	Application is recognized as a CD writing app. (Optional) Series of FileReads from one fileHandle, followed by a series of CDWrite events with the same process. May need to compare filenames, otherwise one read will exhaust all the writes. Alternately, all read files are lumped together with one large burn event. Or perhaps the first read of a new file after the last read from the previous file is the start of the next burn event.	Process
FileLeftThroughNetworkPort	FileRead, TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	An overlapping stream of FileReads interspersed with Inbound and Outbound network events. All the network events should be for the same port (?) and to a destination NOT on localhost. All the network events should be for the same protocol.	Thread

Fig. 5A

Aggregate Event Definitions

Event Name	Constituent Event Types	Pattern	Scope
EmailFile	FileRead, TCPIPInbound, TCPIPOutbound, (other protocols???)	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be an email program. May place constraints on the ports, since many emailers use certain well defined ports for SMTP, POP etc.	Process
InstantMessenger	FileRead, TCPIPInbound, TCPIPOutbound, (other protocols???)	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be used for Instant Messenger. May place constraints on the ports.	Process
P2PApp	FileRead, TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Constrain the application name to be one of those known to be a P2PApp. Multiple ports will be used; some or all of them may have constraints. May constrain the protocol per app or per instance. Similar to FileLeftThroughNetworkPort as concerns interleaved file reads.	Process
FTPFile	FileRead, FileWrite, ??? (TCPIPInbound, TCPIPOutbound)	May want to split into two events, one for reading and one for writing. Constrain to the common FTP port, unless the app is known by name to be an FTP client. Like FileLeftThroughNetworkPort, look for interleaved reads and network events, or interleaved writes and network events.	Process
RemoteAccess	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Do not incorporate FileRead events. Several ports may be used. Look for known image names of remote apps.	Process
TunnelOut	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	All events use same protocol. Only two processes used. Two different apps and four ports are used. One of the ports is remote. Event 1: The first app sends outbound from local port 1 to local port 2. Event 2: The second app (the tunneler) receives inbound from local port 1 to local port 2. Event 3: The tunneler also sends from local port 3 to remote port 4. Both events of the tunneler share the same thread (probably).	Login
TunnelIn	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	All events use same protocol. Only two processes used. Two different apps and four ports are used. One of the ports is remote. Event 1: The first app (the tunneler) receives inbound from remote port 1 to local port 2. Event 2: The tunneler sends outbound from local port 2 to local port 3. Event 3: The second app also receives inbound from local port 3 to local port 4. Both events of the tunneler share the same thread (probably).	Login
TunnelInOut	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Multiple protocols may be used. More research needed. More than three ports are used.	Login

FIG. 5B

Aggregate Event Schemas

Event Name	Constituent Event Types	Pattern	Scope
FileLeftThroughTunnel	FileRead, TunnelOut	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads involving a process that is participating in a TunnelOut event. If more than one file is read, the source destination will be a count of the files read.	Login?

FIG. 5C

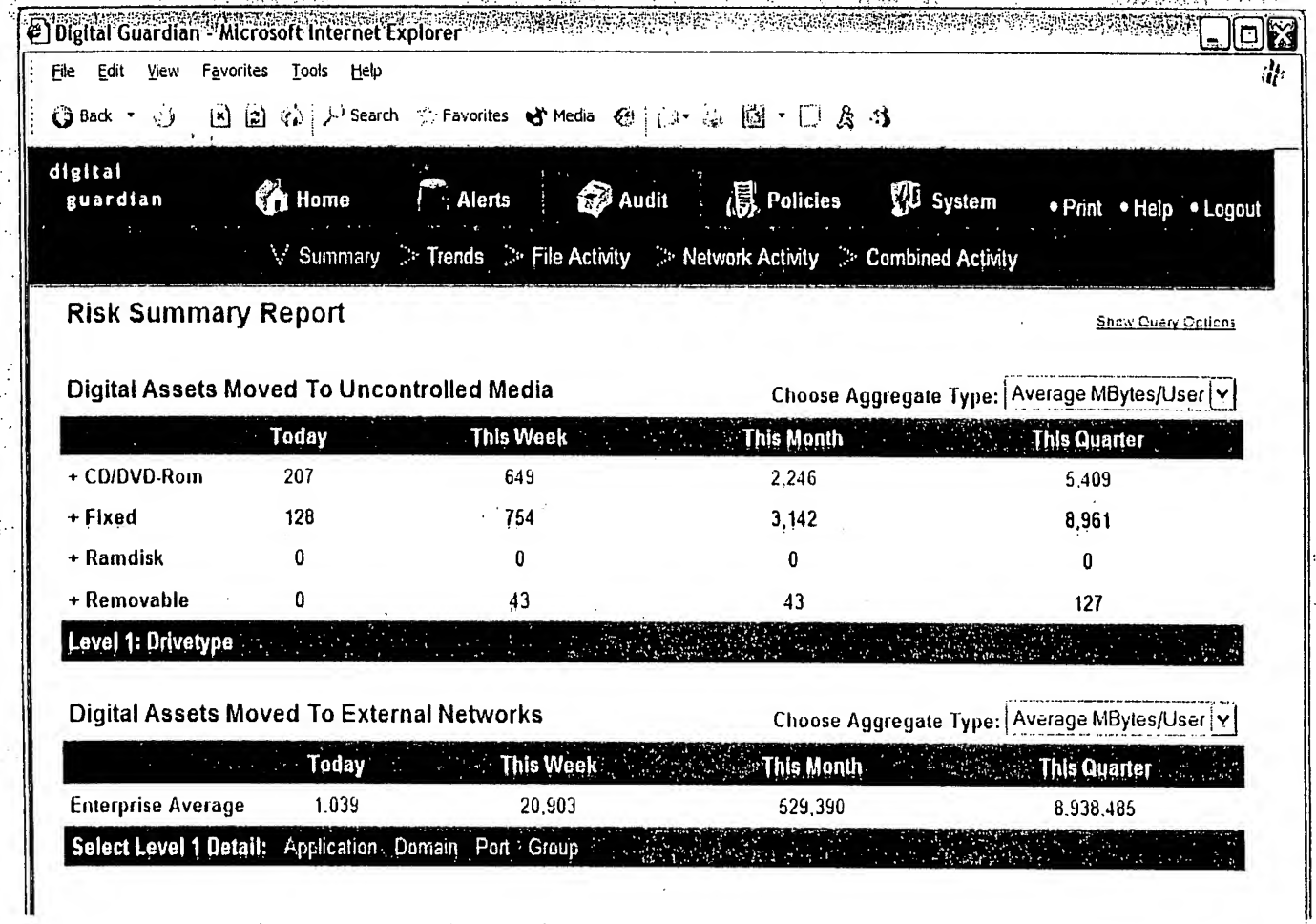
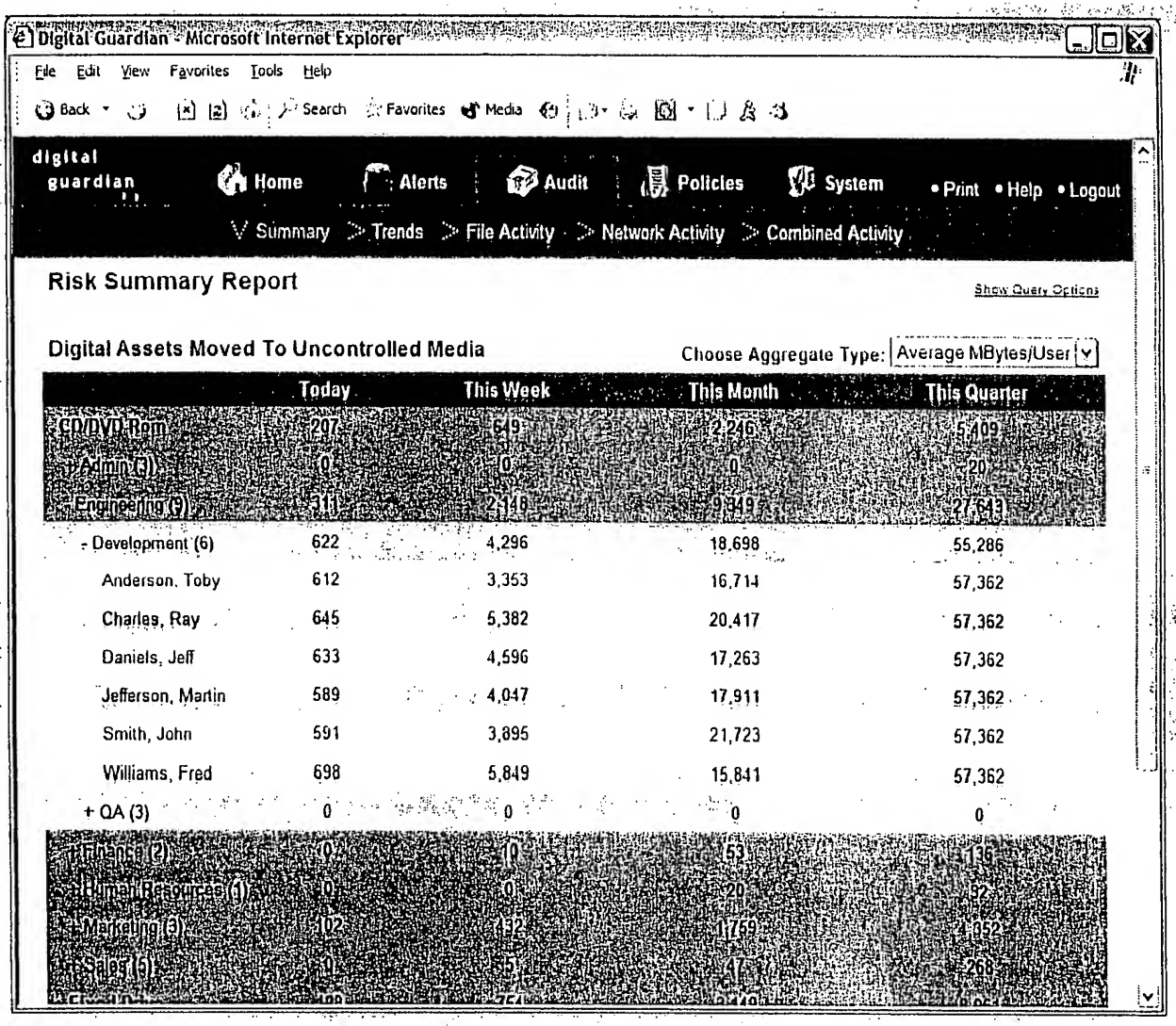


FIG. 6A

BEST AVAILABLE COPY

BEST AVAILABLE COPY



	Today	This Week	This Month	This Quarter
CD/DVD Rom	207	649	2,246	5,409
Admin (3)	0	0	0	20
Engineering (9)	511	2,146	9,349	27,649
- Development (6)	622	4,296	18,698	55,286
Anderson, Toby	612	3,353	16,714	57,362
Charles, Ray	645	5,382	20,417	57,362
Daniels, Jeff	633	4,596	17,263	57,362
Jefferson, Martin	589	4,047	17,911	57,362
Smith, John	591	3,895	21,723	57,362
Williams, Fred	698	5,849	15,841	57,362
+ QA (3)	0	0	0	0
Finance (2)	0	10	53	1136
Human Resources (1)	0	0	20	82
Marketing (3)	102	432	1759	4852
Sales (6)	0	5	47	268

FIG. 6B

BEST AVAILABLE COPY

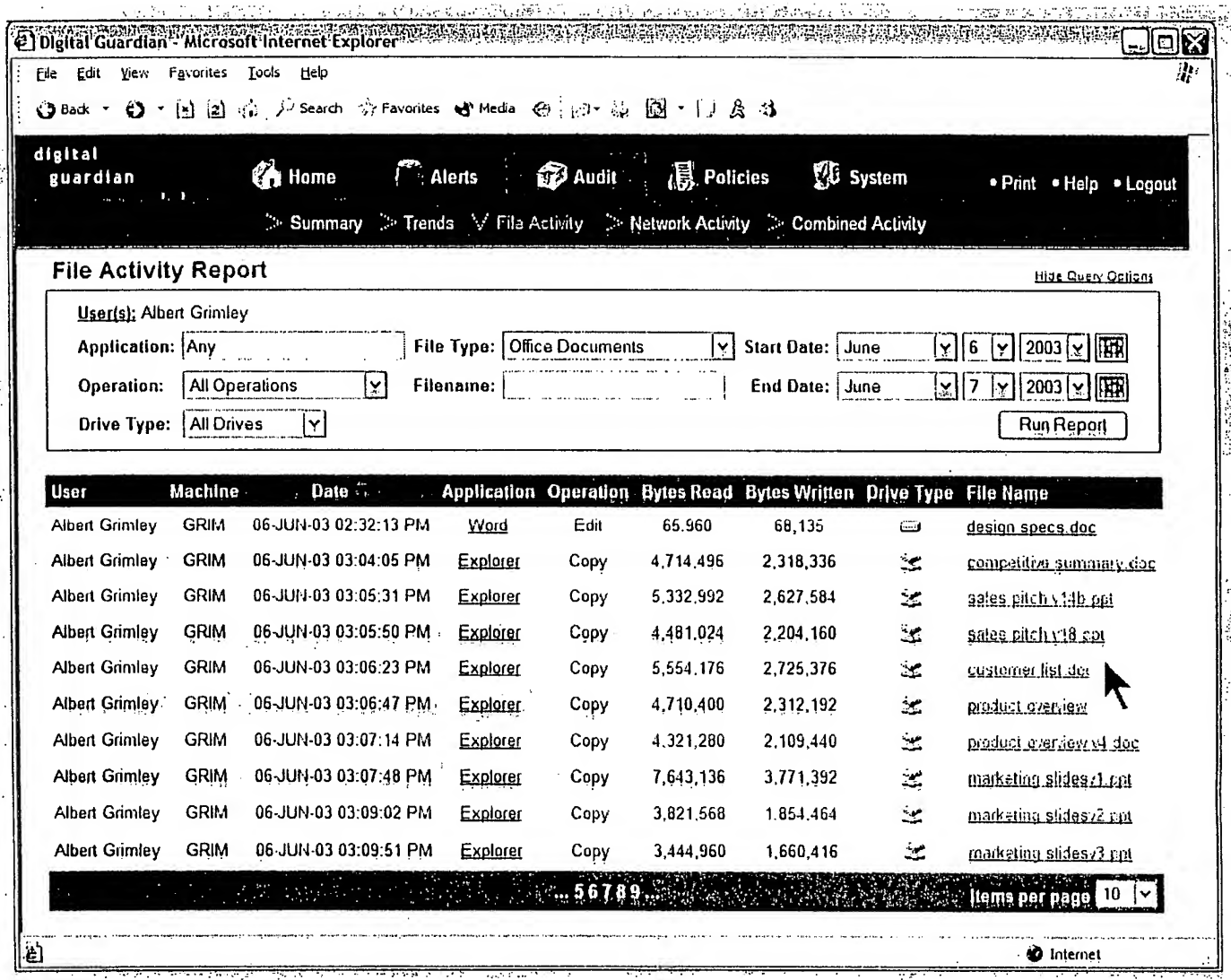


FIG. 6C

BEST AVAILABLE COPY